3. SYSTEM ARCHITECTURE

A. DESIGN PRINCIPLES

Certain principles should guide the design of the portal. As the underlying technologies might change, these principles should be upheld to ensure that future deliverables meet the goals and best practices initially set for the portal. These principles (Figure 4) are

- ***User-Centered Design***: Information must be presented at appropriate level for target audience and usability will be a key design and testing criteria.
- ***Platform Independence***: End user devices shall be platform, operating system, and browser independent. Current end user devices include Windows, Mac, Unix, Palm, and cell phones.
- ***Open***: Users will be distributed across the globe and include NASA employees, external partners, other Government agencies, international partners, and the public.
- ***Modular***: Components from multiple vendors can be swapped in/out; external content and applications will plug in.
- ***Leadership***: Promote a common portal approach across the Agency.
- ***Security***: All users will be authenticated and assigned into one or more groups based on their authorized role(s); information must be protected against unauthorized access or modification.
- ***Standards Based***: Leverage ubiquitous Internet standards and directions.
- ***Integrated with NASA Infrastructure***: Build to easily integrate into existing Center architectures and policies.

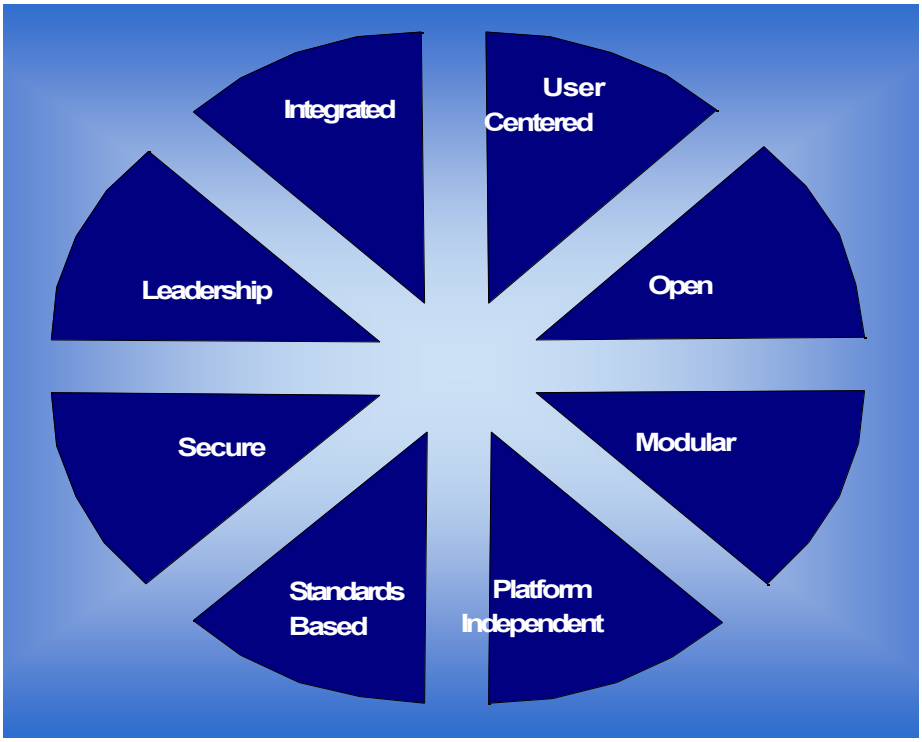

Figure 4. Portal design principles

B. USER INTERFACE

In applying these principles to the portal's user interface, it is critical to reinforce this portal as the user's single entry point. Each user can customize the content and layout to maximize their own efficiency; however, the goals for the generic user interface should include:

- Follow *NASA Web Best Practices*[4] as appropriate
- Provide a consistent look and feel, including the use of the NASA logo, privacy statement, search function, and contact information
- Interface design is about visual guidance. How navigation options are presented is closely tied to how usable they are. If they are hidden, difficult to find, look too much like text, or are otherwise visually confusing, users will have trouble navigating.
- Support easy and efficient navigation
- Be consistent in the placement and design of navigation elements for the generic portal. Users have the right to expect navigation buttons and bars to show up in the

[4] *NASA Web Best Practices*, December 2000, http://nasa-wbp.larc.nasa.gov/

same place every time. Consistency builds the user's trust and enhances the quality of the experience.

- Do not violate expected browser behaviors that users have come to know and trust. For instance, they have come to expect that their browser's back button will always work a certain way and to break this rule without a significant reason is a breach of usability.
- Provide a Home button on every internal page
- Provide overview and frequently asked question (FAQ) pages to give the user background information on the technology and their choices within the system
- Provide e-mail contacts and other points of reference for additional help (such as a Help Desk)
- Provide online help that is contextual and easily available
- Usability testing should be conducted to ensure ease of task completion and resolve any outstanding issues related to key points in portal functionality
- Users should be able to complete required tasks easily. These might include editing data channel content and layout

C. HARDWARE, SOFTWARE, AND NETWORK ARCHITECTURE

Portals can be divided into four layers as depicted in Figure 5. NASA should take an architectural view of portals by defining services at each layer, rather then focusing on the purchase of a single vendor monolithic product to meet all of our requirements.

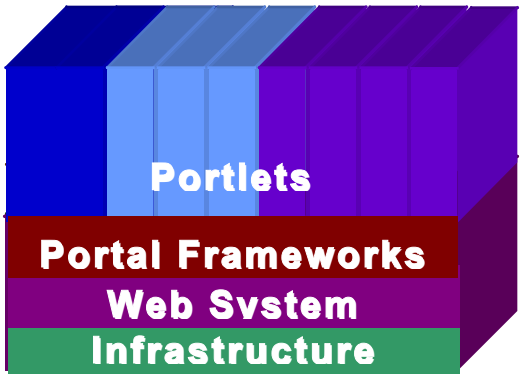

Figure 5. Portal architecture (taken from MetaGroup)

1. Layer 1: Infrastructure

Common infrastructure layer components required to enable a portal are: networking, directory services, email, security (authorization and authentication), end user devices, databases, and enterprise application integration (EAI) services. The NASA networking service, email, and end user devices are ready to support a NASA portal today. Other areas of the NASA infrastructure are not necessarily ready to support a portal, in particular NASA does not have an application-ready corporate directory, nor do we have a fully deployed authentication service that can serve all NASA employees, external partners, and public users.

The portal should be attached to a dedicated high-speed network (e.g. switched Gigabit Ethernet) to ensure optimum performance. Connectivity to the NASA network will be dependent on whether the portal is hosted in an external outsourced environment or at a NASA Center. Assuming external hosting, connectivity to NASA networks will be via in-place Internet connections.

End user device support will include all devices and software defined in NASA STD 2804/2805. Further, flexibility to support emerging mobile devices such as PalmOS and cell phone systems is highly desirable.

Authentication will be enabled by a best practice capability already deployed to thousands of NASA employees within several centers and mission areas. The capability provides two-factor authentication using a hardware token and is based on the RSA SecurID product. The authentication service will be provided by the Secure Nomadic Access (SNA) project.

NASA does not have an application-ready corporate directory service, so for this functionality the portal will use the directory and or membership services provided within the portal framework.

2. Layer 2: Web System Services

The web system services layer is a specific part of the infrastructure that pertains solely to the Web, and is a key enabler of portal systems. Web system services consist of business logic management and data repository access—or what is commonly referred to as “application server” software. Web servers are another key component of the web system services layer. NASA does not have any preferred corporate application server or web server software at this time. This is expected to be addressed by the Web Management Team.

3. Layer 3: Portal Framework

The portal framework is commonly packaged into a commercial "portal" product and consists of components for personalization, profiling, profile management, metadata/taxonomy, content management, access control, and activity tracking. In some cases, some of these components are done by external best of breed services, the most common example being content management.

The portal framework includes an API for plugging external components into it. Many portals also include connectors for easy integration of popular applications in categories such as enterprise resource planning (ERP) and collaboration. Portal application integration capabilities are beginning to overlap with enterprise application integration (EAI) functions (EAI is a separate class of vendor products).

4. Layer 4: Portlets

Portlets are external applications and repositories that you want to link into the portal. External applications that may be desirable to link into a NASA portal include: email systems, collaboration systems, project management systems, content repositories, and ERP systems (e.g. IFMP modules). EAI style connectors are beginning to be seen in portal framework products, enabling integration with portlets.

Based on this discussion, we can see a high-level architecture for the NASA portal as depicted in Figure 6.

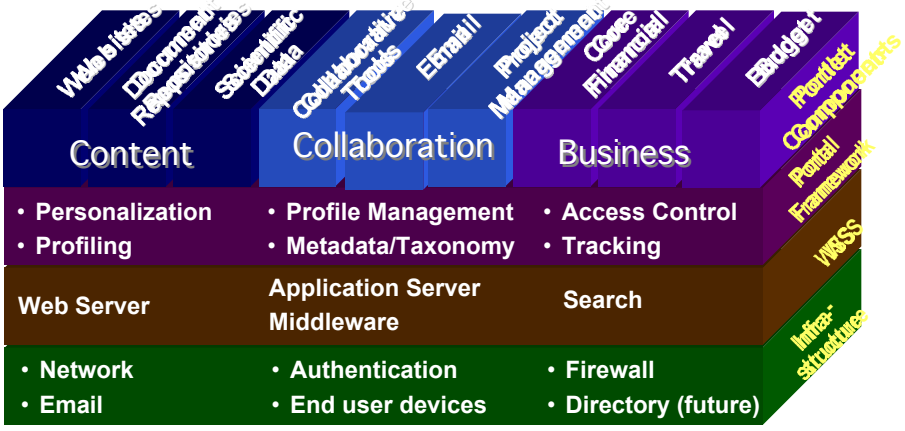

Figure 6. NASA portal architecture

D. SECURITY SYSTEM AND ACCESS CONTROLS

There are many documented threats to our information systems that must be mitigated by policies, processes, and technology. The portal will follow NPG 2810, which establishes basic IT security requirements for NASA systems. In particular, the NASA portal must protect against:

- Unauthorized access to information or applications
- Unauthorized modification (or defacement) of information
- Denial or degradation of service to customers

To mitigate these threats, the NASA portal must implement the following controls:

- Authentication for all users
  - NASA employees via a two-factor (or strong) method
  - A preference for two-factor (or strong) method for all other users when possible
  - NASA external partners via NPG 2810 compliant passwords
  - Public visitors via simple passwords (chosen by user)
- Role-based access to information
  - Users will be authorized into one or more roles
  - Each role will form a group of users
  - Example roles could include
    - NASA employee
    - NASA management
    - Support service contractor
    - External partner
    - Member of project X
    - Public (student, media, etc.)
- Information access control
  - All information objects will have access control lists (of groups and/or individuals)
  - Read/write/delete object privileges will be available
- Information security considerations will be part of portal information hierarchy and taxonomy design so that access control is enabled
- Firewall

E. STANDARDS

There is no generic portal API or other standards in place in the portal industry and none are expected in the next 2 years. However, there are standards we recommend for:

- Connecting portal to infrastructure components include: LDAP (directory access), POP, and IMAP (email store access), and HTTP (end user device access).
- Connecting portal framework to portlets include WebDAV (document/content management access) and enterprise application integration (EAI) products.
- XML can be used in several areas such as the portal API and metadata management, but payloads are proprietary. XML can also be used for access to the emerging area of "Web Services," which is a method for applications to expose coarse-grained services via industry standard protocols (e.g., SOAP and UDDI). Web services provide system-to-system communications only (not for presentation).

We have a preference for a Java programming environment (de facto standard) due to its platform portability.